REMARKS

This Application has been carefully reviewed in light of the Office Action mailed May 17, 2007. Claims 1-34 were pending in the Application. In the Office Action, Claims 1-34 were rejected. Claims 1-34 remain pending in the Application. Applicant respectfully requests reconsideration and favorable action in this case.

In the Office Action, the following actions were taken or matters were raised:

SECTION 103 REJECTIONS

Claims 1-34 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,764,772 issued to Kaufman et al. (hereinafter "*Kaufman*") in view of U.S. Patent No. 6,728,378 issued to Garib (hereinafter "*Garib*"). Applicant respectfully traverses this rejection.

Of the rejected claims, Claims 1, 11, 19 and 27 are independent. Independent Claim 1, for example, recites: "generating a character string at a sender," "generating a hash key using the character string and a private key," "encrypting the data using the hash key" and "transmitting an identification key associated with the sender, the character string, and the encrypted data from the sender to a recipient." (emphasis added). Applicant respectfully submits that the proposed combination of references does not disclose, teach or suggest all claim limitations of independent Claim 1.

Kaufman appears to disclose that a message to be transmitted to an intended recipient is encrypted using a secret key (*Kaufman*, column 7, lines 1-56, column 8, lines 51-58). *Kaufman* also appears to disclose that the secret key is concatenated with a bit string or "salt," and that the secret key and "salt" are encrypted using a public key of the intended recipient (*Kaufman*, column 7, lines 1-56, column 8, lines 51-58). *Kaufman* also appears to disclose that the encrypted secret key and "salt" and the encrypted message are transmitted to the intended recipient such that, when the message is received by the intended recipient, the recipient decrypts the encrypted secret key with the recipient's private key, thereby providing the recipient with the secret key for decrypting the message (*Kaufman*, column 7, lines 1-56, column 8, lines 51-58). Additionally, because the "salt" is included in the portion encrypted with the recipient's public key, the recipient also obtains the "salt." (*Kaufman*, column 8, lines

51-58). *Kaufman* appears to indicate that the "salt" is used by the recipient (in combination with other values) as a mechanism to verify that various portions or fields of the message have been encrypted properly, not deleted, etc. (*Kaufman*, column 8, line 58 to column 9, lines 1-15).

The Examiner appears to rely on *Garib* for purportedly teaching encrypting a message using a hash value (Office Action, page 4). Thus, based on the purported teaching of *Garib*, the Examiner appears to assert that instead of encrypting the message in *Kaufman* with the secret key of *Kaufman*, it would have been obvious to encrypt the message in *Kaufman* with a hash value of the secret key and the "salt" of *Kaufman* (Office Action, page 4). Applicant respectfully disagrees. *Kaufman* appears to disclose that the secret key is a random number which is generated for each message (*Kaufman*, column 7, lines 5-8, figure 1). *Kaufman* also appears to disclose that the "salt" is a randomly generated number (*Kaufman*, column 7, lines 45-47). Thus, according to the Examiner's reasoning, the *Kaufman* message would be encrypted by first generating a random number (i.e., the "secret key"), then generating another random number (i.e., the "salt") to concatenate with the first random number, thereby yielding yet another random number, then generating a hash of the random number and encrypting the message with the hash value. Thus, the process proposed by the Examiner clearly includes repetitive and redundant operations that yield no additional benefit. Thus, Applicant respectfully submits that there is no motivation or suggestion to combine purported reference teachings as proposed by the Examiner.

In the Office Action, as a basis for combining purported reference teachings, the Examiner appears to assert that the proposed combination would yield greater "integrity" and "confidentiality" of the message (Office Action, page 4). Applicant respectfully disagrees. *Kaufman* appears to disclose at least two levels of security for a transmitted message (e.g., encrypting the message using a secret key, and then encrypting the secret key with a public key of the intended recipient). The process proposed by the Examiner would appear to result in only a single layer of security, namely, encrypting the message with a hash value. Thus, for at least this reason also, Applicant respectfully submits that there is no motivation or suggestion to combine purported reference teachings as proposed by the Examiner. In fact, for at least the above reason, *Kaufman* appears to teach away from the proposed modification.

Additionally, in the Office Action, the Examiner asserts that the proposed modification would yield greater "integrity" and "confidentiality" of the message because the secret key of *Kaufman* would not be sent to a recipient (Office Action, page 4). Applicant respectfully disagrees. *Garib* appears to disclose that an account holder or bank customer/client establishes a password that the bank uses to create a password hash value (*Garib*, column 11, lines 16-43, column 12, lines 16-45). *Garib* appears to disclose that the bank discards the password and subsequently uses the password hash value to encrypt messages (e.g., account statements) that are sent to the bank customer/client (*Garib*, column 11, lines 16-43, column 12, lines 16-45). *Garib* further discloses that the bank also transmits to the bank customer/client along with the encrypted bank statement a script or applet that contains a decryption program that automatically launches upon receipt by the bank customer/client and prompts the bank customer/client user for his/her password, which is then used to obtain the password hash value and decrypt the encrypted message (*Garib*, column 11, lines 16-43, column 12, lines 16-45). Thus, *Garib* also relies on security-related information that is transmitted to the recipient that is used and/or needed to decrypt the encrypted message. Accordingly, Applicant respectfully submits that the proposed combination would not yield any greater "integrity" and "confidentiality" of the message as asserted by the Examiner. Therefore, for at least these reasons, Applicant respectfully submits that there is no motivation or suggestion to combine purported reference teachings as asserted by the Examiner, and that Claim 1 is patentable over the cited references.

Independent Claim 11 recites: "receiving a character string from a sender," "receiving an identification key from the sender," "receiving encrypted data from the sender," "<u>determining a private key associated with the sender using the identification key,</u>" and "<u>decrypting the encrypted data using the private key</u> and the character string" (emphasis added). Applicant respectfully submits that the proposed combination of references does not disclose, teach or suggest all claim limitations of independent Claim 11. In the Office Action, the Examiner appears to assert that *Kaufman* teaches all of the limitations of Claim 11 except for using a hash value to encrypt the data, which the Examiner relies on *Garib* to purportedly disclose (Office Action, page 8). Applicant respectfully disagrees. For example, *Kaufman* appears to disclose that a message is encrypted using a secret key, and then the secret key in encrypted using a public key corresponding to the recipient of the message such that the recipient uses the recipient's private key to decrypt upon receipt (*Kaufman*, column 7, lines 1-56, column 8, lines 51-58). Thus, *Kaufman* does not disclose or even suggest "determining a private key associated with the sender using the identification key" and "decrypting the encrypted data using the private key" as recited by Claim 11. To the contrary, no identification information associated with the sender appears to be used or needed in *Kaufman* at least because the recipient uses his/her own private key to perform a decryption process. Moreover, at least for the reasons discussed above in connection with independent Claim 1, there is no motivation or suggestion to modify the cited references as proposed by the Examiner to use a hash value as purportedly taught by *Garib*. In fact, at least *Kaufman* appears to teach away from the modification proposed by the Examiner. Therefore, for at least these reasons, Applicant respectfully submits that Claim 11 is patentable over the cited references.

Independent Claim 19 recites: "a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string and a private key," "an encryption engine stored in the memory and executable by the processor, the encryption engine adapted to encrypt the data using the hash key," and "wherein the processor is adapted to transmit the encrypted data, an identification key related to the private key, and the character string to a recipient." (emphasis added). For at least the reasons indicated above with respect to independent Claim 1, Applicant respectfully submits that the proposed combination of references fails to disclose, teach or suggest the limitations recited by Claim 19. Accordingly, Applicant respectfully submits that independent Claim 19 is patentable over the proposed combination of references.

Independent Claim 27 recites: "a processor adapted to receive encrypted data, an identification key, and a character string from a sender", "a memory coupled to the processor", "a relational database stored in the memory and accessible by the processor, the relational database relating the identification key to a private key", and "a decryption engine stored in the memory and executable by the processor adapted to receive, the decryption engine adapted to decrypt the encrypted data using the character string and the private key." (emphasis added). For at least the reasons indicated above in connection with independent Claims 1 and 11, Applicant respectfully submits that the proposed combination of references fails to disclose, teach or suggest the limitations recited by Claim 27. Therefore, for at least these reasons, Applicant respectfully submits that independent Claim 27 is patentable over the proposed combination of references.

Claims 2-10, 12-18, 20-26 and 28-34 depend respectively from independent Claims 1, 11, 19 and 27. For at least the reasons discussed above, independent Claims 1, 11, 19 and 27 are in condition for allowance. Therefore, Claims 2-10, 12-18, 20-26 and 28-34 are also in condition for allowance, and Applicant respectfully requests that the rejection of Claims 1-34 be withdrawn.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicant has overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By: James L Baudino
James L. Baudino
Reg. No. 43,486

Date: August 17, 2007

Correspondence to:

Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400